REMARKS

Reconsideration of the present application is respectfully requested in light of the above amendments to the claims and the foregoing remarks.

Status of the Claims

Applicants have amended Claims 1, 4, 6, and 49 herein. Applicants have canceled Claims 2, 3, 7-48, and 50-59 without prejudice to, or disclaimer of, the subject matter recited therein. Applicants have added new Claims 60-75. Upon entry of this amendment, Claims 1, 4, 6, 49, and 60-75 are pending in the present application. Claims 1, 49, 66, and 71 are the independent claims. The amendments to the claims and new claims are fully supported by the specification and do not include new matter.

Unless explicitly stated otherwise, none of the amendments to the claims were made for reasons substantially related to the statutory requirements for patentability. Furthermore, unless otherwise stated, the amendments to the claims were made simply to make express that which had been implicit in the claims as originally worded and therefore are not narrowing amendments that would create any prosecution history estoppel.

Claim Rejections

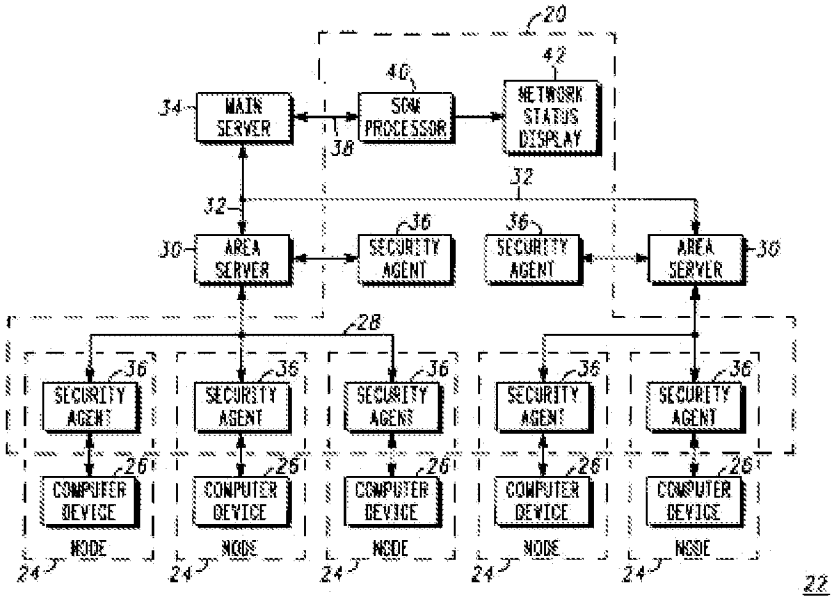
In the Decision on Appeal mailed February 11, 2010, the Examiner's rejections of Claims 1-59 were affirmed. In the Final Office Action mailed on November 11, 2006, the Examiner rejected Claims 27-29 and 31-32 under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,088,804 to Hill et al. (hereinafter "*Hill*"). The Examiner also rejected Claims 1-26, 30, and 33-59 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Hill* in view of U.S. Patent No. 6,775,657 to Baker (hereinafter "*Baker*"). Claims 2, 3, 7-48, and 50-59 are canceled herein. Accordingly, the rejection with regard to Claims 2, 3, 7-48, and 50-59 has been rendered moot. Applicants respectfully offer the following remarks to traverse the rejection of independent Claims 1 and 49.

Independent Claim 1

The rejection of Claim 1 is traversed. Applicants submit that the combination of *Hill* and *Baker* fails to teach, suggest, or make obvious all of the elements of independent Claim 1, as

amended. In particular, the combination fails to teach, suggest, or make obvious the features of (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data as result data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a location of a security event, a source of security event, and a destination address of the security event; and (3) the computer filtering the collected security event data using the one or more user-configurable variables to produce the result data for the event data report.

As Applicants understand, the *Hill* reference describes a dynamic network security system (20) that responds to a security attack on a computer network (22) having a multiplicity of computer nodes (24). The security system (20) includes a plurality of security agents (36) that concurrently detect occurrences of security events on associated computer nodes (24). A processor (40) processes the security events that are received from the security agents (36) to form an attack signature of the attack. A network status display (42) displays multi-dimensional attack status information representing the attack in a two dimensional image to indicate the overall nature and severity of the attack. See Figure 1 of the *Hill* system reproduced below.



As shown in Figure 3 of the *Hill* reference below, a database (48) maintains the simulated attack information for a plurality of simulated attacks (52). Each of the simulated attacks (52) is a prediction of an attack type that may occur on network (22). Simulated attacks (52) are

generated by an operator and stored in database (48). Each simulated attack (52) contains a training signature (53) that is defined by a plurality of security events (50) of at least one security event type (56). Security events (50) are presented in database (48) in a column (58) as a percentage of security events per event type.

In addition to security event types (56) and percentage of security events (50) per event type in column (58), training signatures (53) include location identifiers (60). Location identifiers (60) identify the nodes (24) in network (22) where security events may take place. Location identifiers (60) are important for ascertaining an attack severity (61) for each of simulated attacks (52). Attack severity (61) is a level of security breach that one of simulated attacks (52) could cause computer network (22).

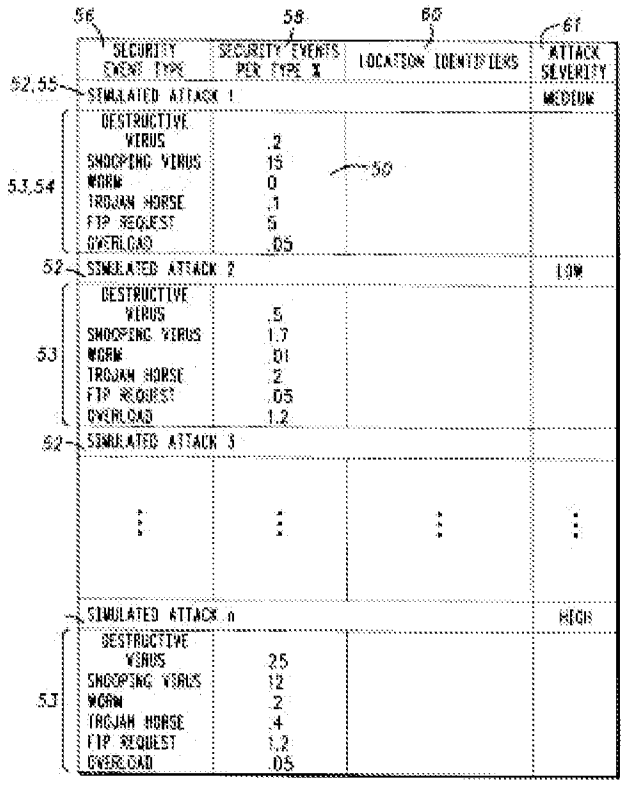


FIG. 3

As shown in Figure 7 of the *Hill* reference below, a network status display (42) displays multi-dimensional attack status information in a two dimensional image to indicate the overall nature and severity of an attack. The network status display (42) presents a display map (66) and an attack status information list (108) showing security event type (56) and location identifiers

(60) for an example attack (92). The network status display (42) also presents an attack signature log (110) which provides current and historical perspective on a given attack record at various sample times. The attack signatures in log (110) are the text equivalent of the two dimensional image as highlighted in display map (66). In addition, the network status display (42) includes an attack mitigation list (112) which is a catalogue of actions that a network manager may take in order to mitigate the example attack (92).

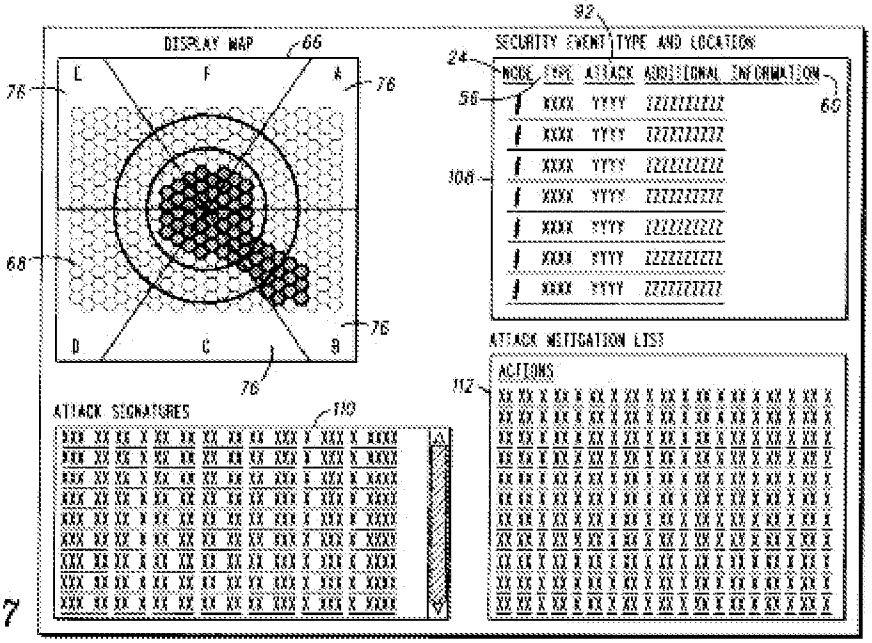


FIG. 7

In summary, the *Hill* reference teaches generating simulated attacks that may occur on the network. These simulated attacks comprise training signatures that define what types of security events are present in each attack. In response to the simulated attacks, the system in the *Hill* reference can subsequently be trained to detect and respond to actual security attacks by monitoring and analyzing the network traffic data. Subsequently, in response to an actual security attack, the system in the *Hill* reference can respond with an action that corresponds to a simulated attack that is stored in the database. Furthermore, in response to an actual security attack, the *Hill* reference can present a display map containing attack information.

Therefore, the *Hill* reference fails to teach the following features recited by Claim 1: (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data as result data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a location of a

security event, a source of security event, and a destination address of the security event; and (3) the computer filtering the collected security event data using the one or more user-configurable variables to produce the result data for the event data report. The *Hill* reference merely teaches displaying (1) multi-dimensional attack status information showing security event type and location identifiers for an example attack; (2) an attack signature log which provides current and historical perspective on a given attack record at various sample times; and (3) an attack mitigation list which is a catalogue of actions that a network manager may take in order to mitigate the example attack.

The *Hill* reference fails to teach or suggest configurable event data reports that identify a portion of security event data. Instead, the *Hill* reference merely discloses that "[n]etwork status display 42 is configured to display attack status information representative of an attack in response to the attack signature." *See Hill*, col. 5:10-12. Simply displaying attack status information is not the same as displaying an event data report comprising result data produced by filtering security event data using user-configurable variables that are selected via a user interface.

Further, the network status display of the *Hill* reference works in cooperation with a self-organizing map ("SOM") processor to display attack status information. This SOM processor of the *Hill* reference does not filter security event data using user-configurable variables. Instead, the SOM processor is trained using a plurality of simulated attacks to map a display map. Although the *Hill* reference discloses that the simulated attacks "are generated by an operator," the *Hill* reference does not disclose or suggest that the simulated attacks are generated by receiving a selection of one or more user-configurable variables operable for filtering security event data to render a portion of the security event data. *See Hill*, col. 5:40-42.

Similarly, the *Baker* reference fails to teach, suggest, or make obvious these features of amended Claim 1. Accordingly, Applicants submit that Claim 1 is patentable over the combination of references cited by the Examiner.

Independent Claim 49

The rejection of Claim 49 is traversed. Applicants submit that the combination of *Hill* and *Baker* fails to teach, suggest, or make obvious all of the elements of independent Claim 49, as amended. In particular, the combination fails to teach, suggest, or make obvious the features of (1) the computer presenting a user interface via the display for configuring an event data

report that identifies a portion of the security event data as result data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event; and (3) the computer filtering the stored security event data using the one or more user-configurable variables to produce the result data for the event data report.

As described above with reference to the discussion of independent Claim 1, the combination of *Hill* and *Baker* fails to teach, suggest, or make obvious a computer presenting a user interface for configuring an event data report that identifies a portion of security event data; or a computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data. Furthermore, as described above with reference to the discussion of independent Claim 1, the combination of *Hill* and *Baker* fails to teach, suggest or make obvious the computer filtering the collected security event data using the one or more user-configurable variables to produce the result data for the event data report. Therefore, the combination of *Hill* and *Baker* fails to teach, suggest, or make obvious the features of: (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data as result data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event; and (3) the computer filtering the stored security event data using the one or more user-configurable variables to produce the result data for the event data report.

Accordingly, Applicants submit that Claim 49 is patentable over the combination of references cited by the Examiner.

Independent Claims 66 and 71

New independent Claims 66 and 71 recite similar features as described above with reference to the discussion of Claims 1 and 49, respectively. Therefore, Applicants submit that new independent Claims 66 and 71 are likewise patentable over the combination of *Hill* and *Baker*.

Dependent Claims

Each of Claims 4, 6, 60-65, 67-70, and 72-75 depends directly or indirectly from one of the independent claims discussed above. Accordingly, for at least the reasons discussed above with respect to the independent claims, Applicants submit that the dependent claims are likewise patentable over the documents cited by the Examiner. The dependent claims also recite additional features that further define the claimed invention over at least the documents cited by the Examiner. Applicants submit that the documents cited by the Examiner do not disclose, teach, suggest, or make obvious integrating any of those additional features into the presently claimed invention. Accordingly, Applicants request separate and individual consideration of each dependent claim.

No Waiver

Applicants have not addressed each specific rejection of the independent and dependent claims because Applicants submit that the independent claims are allowable, as discussed above. Applicants have not acquiesced to any such claim rejections and reserve the right to address the patentability of any additional claim features in the future.

CONCLUSION

The foregoing is submitted as a full and complete response to the Decision on Appeal mailed on February 17, 2010. Applicants submit that this application is in condition for allowance and respectfully requests such action. If any issues exist that can be resolved with an Examiner's Amendment or a telephone conference, please contact Applicants' undersigned attorney at 404.572.2888.

Respectfully submitted,
KING & SPALDING LLP
By:

/W. Scott Petty/

W. Scott Petty
Registration No. 35,645

King & Spalding LLP
1180 Peachtree Street, N.E. - 34th Floor
Atlanta, Georgia 30309
Telephone: (404) 572-4600